Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Summary of Local Government and Court Audit Findings - Information Security Controls

User Access Management	Access to certain systems is not adequately restricted. The user access of former employees is not disabled timely. Policies and procedures are not fully established or documented to ensure areas housing information technology resources are properly controlled, monitored, and restricted.
User Authentication	Passwords are not required to be changed on a periodic basis. User accounts and passwords for accessing computers and various systems are shared by users. A password is not required to logon and authenticate access to a computer. Passwords are not required to contain a minimum number of characters.
Security Controls	Inactivity controls have not been implemented to lock a computer or system after a certain period of inactivity. Security controls have not been implemented to lock access to a computer or system after a specified number of unsuccessful logon attempts. Malware or antivirus protection software to detect and eradicate malicious code has not been installed on computer systems.
Backup and Recovery	Data in various systems is not periodically backed up. Data backups are not stored at a secure off-site location. Periodic testing of backup data is not performed. Management has not developed a formal contingency plan to ensure business operations and computer systems can be promptly restored in the event of a disaster or other disruptive incident.
Data Management and Integrity	Data management and integrity controls to guard against the improper modification or destruction of data and information have not been implemented.
Vendor Security	Contracts for software acquired or outsourced from information technology vendors do not always contain security requirements. Security practices used by vendors are not always reviewed.

Because of the nature of this report, no rating is provided.